

Bipartite subspaces having no LOCC-distinguishable bases

John Watrous

Institute for Quantum Information Science and
Department of Computer Science
University of Calgary
Calgary, Alberta, Canada

March 18, 2005

Abstract

It is proved that there exist subspaces of bipartite tensor product spaces that have no orthonormal bases that can be perfectly distinguished by means of LOCC protocols. A corollary of this fact is that there exist quantum channels having sub-optimal classical capacity even when the receiver may communicate classically with a third party that represents the channel's environment.

1 Introduction

One of the main focuses of the theory of quantum information in recent years has been to understand the powers and limitations of *LOCC protocols*. These are protocols wherein two or more physically separated parties possess the ability to perform arbitrary operations on local quantum systems and to communicate with one another, but only classically. The paradigm of LOCC, short for *local operations and classical communication*, provides a setting in which to address basic questions about the nature of entanglement and non-locality, generally viewed as principal characteristics of quantum information.

One question along these lines that has received a great deal of attention is that of *LOCC distinguishability* of sets of states. In the two-party case, the two parties (Alice and Bob) share one of a known orthogonal collection of pure states, and their goal is to determine which of the states it is [1, 2, 3, 4, 6, 5, 9, 10, 13, 14]. In some cases it is possible for Alice and Bob to perform this task without error and in some it is not. For example, the fundamental result of Walgate, et al. [14] establishes that any two orthogonal pure states can be distinguished without error. On the other hand, large sets of maximally entangled states cannot; for instance, if Alice and Bob's systems each correspond to n dimensional spaces, then it is impossible for them to perfectly distinguish $n + 1$ or more maximally entangled states [10]. Other examples of sets of orthogonal states that cannot be perfectly distinguished by LOCC protocols include those of [1] and any set of states forming an

unextendable product basis [2]. These examples demonstrate that entanglement is not an essential feature of LOCC indistinguishable sets of states given that these sets contain only product states.

This paper considers a related question, which is whether there exist subspaces of bipartite tensor product spaces such that no orthonormal basis of the subspace has the property that its elements can be perfectly distinguished by means of an LOCC protocol. Many examples of LOCC-indistinguishable sets fail to give an example of such a subspace in that they span subspaces for which one can easily find a perfectly distinguishable basis. For example, the four Bell states are not perfectly distinguishable by any LOCC protocol, but the space spanned by these states obviously does have a perfectly distinguishable basis—the standard basis. Indeed, *every* subspace of a tensor product space $\mathcal{A} \otimes \mathcal{B}$ for which $\dim(\mathcal{A}) = \dim(\mathcal{B}) = 2$ has a basis whose elements can be perfectly distinguished by some LOCC protocol, and therefore fails to have the property we are considering. We prove, however, that if the dimension of both \mathcal{A} and \mathcal{B} is at least three, then there do exist subspaces of $\mathcal{A} \otimes \mathcal{B}$ with the property that no basis of the subspace is LOCC distinguishable. In particular, it is proved that in the case $n = \dim(\mathcal{A}) = \dim(\mathcal{B})$ for $n \geq 3$, the subspace of dimension $n^2 - 1$ that is orthogonal to the canonical maximally entangled state (or any other fixed maximally entangled state) has this property.

One motive for investigating this property is to identify quantum channels having suboptimal classical corrected capacity with respect to the definition of Hayden and King [8]. More specifically, Hayden and King considered the situation in which a sender transmits classical information over a quantum channel to a receiver, who has the added capability to measure the environment and use the result to correct the channel’s output. This notion of correcting the output of a quantum channel by measuring the environment was considered earlier by Gregoratti and Werner [7], who focused primarily on the quantum capacity of such channels. Based on the result of Walgate, et al. [14], Hayden and King proved that the *classical corrected capacity* of any quantum channel is at least one bit of information. Many natural examples of channels can easily be seen to in fact have *optimal* classical corrected capacity, meaning that the capacity is $\log_2 n$ for n the dimension of the input space, and no examples of channels were previously proved to have less than optimal classical corrected capacity. The existence of subspaces having no LOCC distinguishable bases implies the existence of such channels, even if the definition of Hayden and King is extended to allow two-way communication between the receiver and the environment.

The remainder of this paper is organized as follows. Section 2 discusses notation and background information, Section 3 contains a proof of the main result of the paper, which is that there exist subspaces of bipartite tensor product spaces having no LOCC distinguishable bases, and Section 4 discusses the implications of this result to classical corrected capacities of quantum channels. The paper concludes with a short list of open questions.

2 Preliminaries

Basic notation

This paper will use standard mathematical notation rather than Dirac notation to represent vectors and linear mappings. All vector spaces discussed in this paper are assumed to be finite dimensional

complex vector spaces. The standard basis of a vector space \mathcal{X} of the form $\mathcal{X} = \mathbb{C}^n$ is $\{e_1, \dots, e_n\}$, where e_i is the elementary unit vector defined by $e_i[j] = \delta_{ij}$. The space of linear mappings from a space \mathcal{Y} to a space \mathcal{X} is denoted $L(\mathcal{Y}, \mathcal{X})$, and we write $L(\mathcal{X})$ as shorthand for $L(\mathcal{X}, \mathcal{X})$ and \mathcal{X}^* as shorthand for $L(\mathcal{X}, \mathbb{C})$. If $\mathcal{X} = \mathbb{C}^n$ and $\mathcal{Y} = \mathbb{C}^m$, then elements of \mathcal{X} are identified with n dimensional column vectors, elements of \mathcal{X}^* are identified with n dimensional row vectors, and elements of $L(\mathcal{Y}, \mathcal{X})$ are identified with $n \times m$ matrices in the typical way. For $x \in \mathcal{X}$ we let $\bar{x} \in \mathcal{X}$ and $x^\top, x^* \in \mathcal{X}^*$ denote the entry-wise complex conjugate, transpose, and conjugate transpose of x , and similar for linear mappings; $\bar{X} \in L(\mathcal{Y}, \mathcal{X})$ and $X^\top, X^* \in L(\mathcal{X}, \mathcal{Y})$ denote the entry-wise complex conjugate, transpose, and conjugate transpose of $X \in L(\mathcal{Y}, \mathcal{X})$. The usual inner products on \mathcal{X} and $L(\mathcal{Y}, \mathcal{X})$ are given by $\langle x, y \rangle = x^* y$ and $\langle X, Y \rangle = \text{tr}(X^* Y)$ for $x, y \in \mathcal{X}$ and $X, Y \in L(\mathcal{Y}, \mathcal{X})$. The standard basis of the space $L(\mathcal{Y}, \mathcal{X})$ consists of the mappings $E_{i,j} = e_i e_j^*$ for $1 \leq i \leq n$ and $1 \leq j \leq m$.

The identity operator acting on a given space \mathcal{X} is denoted $I_{\mathcal{X}}$, or just as I when \mathcal{X} is implicit or otherwise understood. It is sometimes helpful to give different names to distinct but otherwise identical spaces; in particular, we assume that $\mathcal{A} = \mathbb{C}^n$ and $\mathcal{B} = \mathbb{C}^n$ are vector spaces referring to Alice's and Bob's systems, respectively, throughout the paper. We define $I_{\mathcal{B}, \mathcal{A}} \in L(\mathcal{B}, \mathcal{A})$ to be the linear mapping that identifies vectors in \mathcal{A} with vectors in \mathcal{B} by identifying the standard bases of these spaces. Often this mapping is used implicitly. For instance, if $a \in \mathcal{A}$ and $b \in \mathcal{B}$ then $\langle a, b \rangle$ is shorthand for $\langle a, I_{\mathcal{B}, \mathcal{A}} b \rangle$, and when $X \in L(\mathcal{A}, \mathcal{B})$ we write $\text{tr}(X)$ to mean $\text{tr}(I_{\mathcal{B}, \mathcal{A}} X)$.

It is convenient when discussing bipartite quantum states to define a linear bijection

$$\text{vec} : L(\mathcal{Y}, \mathcal{X}) \rightarrow \mathcal{X} \otimes \mathcal{Y}$$

by the action $\text{vec}(E_{i,j}) = e_i \otimes e_j$ on standard basis elements, extending by linearity. It is simple to verify that for any choice of linear mappings A , X , and B (for which the product AXB is sensible), the equation

$$(A \otimes B^\top) \text{vec}(X) = \text{vec}(AXB)$$

is satisfied. For $\mathcal{A} = \mathbb{C}^n$ and $\mathcal{B} = \mathbb{C}^n$, the unit vector

$$\frac{1}{\sqrt{n}} \text{vec}(I_{\mathcal{B}, \mathcal{A}}) = \frac{1}{\sqrt{n}} \sum_{i=1}^n e_i \otimes e_i \in \mathcal{A} \otimes \mathcal{B}$$

represents the canonical maximally entangled pure state in the space $\mathcal{A} \otimes \mathcal{B}$. Let $P \in L(\mathcal{A} \otimes \mathcal{B})$ represent the projection onto the space spanned by this vector,

$$P = \frac{1}{n} \text{vec}(I_{\mathcal{B}, \mathcal{A}}) \text{vec}(I_{\mathcal{B}, \mathcal{A}})^*,$$

and let $Q \in L(\mathcal{A} \otimes \mathcal{B})$ denote the projection onto the orthogonal complement of this space,

$$Q = I_{\mathcal{A} \otimes \mathcal{B}} - P.$$

Also let \mathcal{P} and \mathcal{Q} denote the subspaces of $\mathcal{A} \otimes \mathcal{B}$ onto which P and Q project.

Separable measurements and perfect distinguishability

There is no simple characterization known for the set of measurements that can be realized by means of LOCC protocols. For this reason it will simplify matters greatly for us to consider the set of *separable measurements*, which does have a simple mathematical characterization that we now discuss.

Let \mathcal{A} and \mathcal{B} be spaces corresponding to two parties Alice and Bob. A *separable measurement* on $\mathcal{A} \otimes \mathcal{B}$ with possible outcomes $\{1, \dots, N\}$ is a POVM described by a collection

$$\{A_i \otimes B_i : i = 1, \dots, N\} \subset \mathcal{L}(\mathcal{A} \otimes \mathcal{B}).$$

Similar to ordinary POVMs, A_i and B_i must be positive semidefinite operators for each i , and must satisfy

$$\sum_{i=1}^N A_i \otimes B_i = I_{\mathcal{A} \otimes \mathcal{B}}.$$

If we have that each of the operators A_i and B_i has rank equal to one, we will say that the measurement is a *rank one separable measurement*. Any measurement that can be realized by means of an LOCC protocol can be described by a rank one separable measurement in the sense of the following proposition.

Proposition 1. *Suppose that $\{M_k : k = 1, \dots, m\}$ is a POVM that describes the classical output of a given LOCC protocol on $\mathcal{A} \otimes \mathcal{B}$. Then there exists a rank one separable measurement*

$$\{a_i a_i^* \otimes b_i b_i^* : i = 1, \dots, N\}$$

on $\mathcal{A} \otimes \mathcal{B}$ together with a partition $S_1 \cup \dots \cup S_m = \{1, \dots, N\}$, $S_k \cap S_l = \emptyset$ for $k \neq l$, such that

$$M_k = \sum_{i \in S_k} a_i a_i^* \otimes b_i b_i^*$$

for $1 \leq k \leq m$.

The fact that the classical output of any LOCC protocol can be described by a separable measurement is well-known and the proof is routine. It seems to have been first observed by Vedral and Plenio [12] and is discussed further in references [1, 11]. By considering the spectral decomposition of its POVM elements, any separable measurement can easily be further resolved to have rank one as claimed by the proposition. We note that the converse of the theorem is known to be false, as there exist separable measurements that cannot be realized by LOCC protocols [1].

Suppose that $u_1, \dots, u_m \in \mathcal{A} \otimes \mathcal{B}$ is a collection of unit vectors. A separable measurement $\{A_i \otimes B_i : i = 1, \dots, N\}$ may be said to *perfectly distinguish* this collection of vectors if there exists a partition $S_1 \cup \dots \cup S_m = \{1, \dots, N\}$, $S_k \cap S_l = \emptyset$ for $k \neq l$, such that

$$u_k^* \left(\sum_{i \in S_l} A_i \otimes B_i \right) u_k = \delta_{kl}$$

for $1 \leq k, l \leq m$.

Corollary 2. *If Alice and Bob can perfectly distinguish the states u_1, \dots, u_m by means of an LOCC protocol, then there exists a rank one separable measurement*

$$\{a_i a_i^* \otimes b_i b_i^* : i = 1, \dots, N\}$$

that perfectly distinguishes u_1, \dots, u_m .

We also note that, without loss of generality, the measurement in this corollary may be assumed to satisfy the property that $a_i \otimes b_i$ and $a_j \otimes b_j$ are linearly independent for each choice of $i \neq j$.

Unitary equivalence of realizations of completely positive maps

The main result of this paper is applied to the question of channel capacities in Section 4. It will be helpful in that section to have noted the simple fact below concerning realizations of completely positive maps.

Let $\mathcal{T}(\mathcal{X}, \mathcal{Y})$ denote the space of linear mappings of the form $\Phi : \mathcal{L}(\mathcal{X}) \rightarrow \mathcal{L}(\mathcal{Y})$. The *Jamiołkowski isomorphism* is the linear mapping of the form $J : \mathcal{T}(\mathcal{X}, \mathcal{Y}) \rightarrow \mathcal{L}(\mathcal{Y} \otimes \mathcal{X})$ defined by

$$J(\Phi) = \sum_{i,j} \Phi(E_{i,j}) \otimes E_{i,j} = (\Phi \otimes I_{\mathcal{L}(\mathcal{X})})(\text{vec}(I_{\mathcal{X}}) \text{vec}(I_{\mathcal{X}})^*).$$

Proposition 3. *Suppose that $\Phi \in \mathcal{T}(\mathcal{X}, \mathcal{Y})$ is completely positive, and further suppose that \mathcal{Z} is a space and $A, B \in \mathcal{L}(\mathcal{X}, \mathcal{Y} \otimes \mathcal{Z})$ are linear mappings that both realize Φ in the sense that*

$$\Phi(X) = \text{tr}_{\mathcal{Z}} A X A^* = \text{tr}_{\mathcal{Z}} B X B^*$$

for all $X \in \mathcal{L}(\mathcal{X})$. Then there is a unitary operator $U \in \mathcal{L}(\mathcal{Z})$ such that $A = (I \otimes U)B$.

Proof. We have

$$\begin{aligned} J(\Phi) &= (\Phi \otimes I_{\mathcal{L}(\mathcal{X})})(\text{vec}(I_{\mathcal{X}}) \text{vec}(I_{\mathcal{X}})^*) \\ &= \text{tr}_{\mathcal{Z}} (A \otimes I_{\mathcal{X}}) \text{vec}(I_{\mathcal{X}}) \text{vec}(I_{\mathcal{X}})^* (A \otimes I_{\mathcal{X}})^* \\ &= \text{tr}_{\mathcal{Z}} \text{vec}(A) \text{vec}(A)^*, \end{aligned}$$

and so $\text{vec}(A) \in \mathcal{Y} \otimes \mathcal{Z} \otimes \mathcal{X}$ is a purification of $J(\Phi)$. Likewise, $\text{vec}(B)$ is a purification of $J(\Phi)$ as well. It is well-known that two purifications of a given positive semidefinite operator are equivalent up to a unitary operator on the space that is traced out. In the present situation this implies

$$\text{vec}(A) = (I_{\mathcal{Y}} \otimes U \otimes I_{\mathcal{X}}) \text{vec}(B) = \text{vec}((I_{\mathcal{Y}} \otimes U)B)$$

for some unitary operator $U \in \mathcal{L}(\mathcal{Z})$. This is equivalent to $A = (I_{\mathcal{Y}} \otimes U)B$, and so the proposition is proved. \square

3 Two-way indistinguishability

This section contains a proof of the main result of this paper, which is stated in the following theorem.

Theorem 4. *Let $\mathcal{A} = \mathbb{C}^n$ and $\mathcal{B} = \mathbb{C}^n$ for $n \geq 3$. Then there is no basis of the subspace $\mathcal{Q} \subseteq \mathcal{A} \otimes \mathcal{B}$ that is perfectly distinguishable by any LOCC protocol.*

Before giving a formal proof of this theorem, it will be helpful to give a brief sketch of the proof. Recall that the operator

$$Q = I_{\mathcal{A} \otimes \mathcal{B}} - \frac{1}{n} \text{vec}(I_{\mathcal{B}, \mathcal{A}}) \text{vec}(I_{\mathcal{B}, \mathcal{A}})^*$$

is the projection onto the subspace \mathcal{Q} . If $\{u_1, \dots, u_{n^2-1}\}$ is a basis of \mathcal{Q} whose elements are perfectly distinguished by some LOCC protocol, then these elements are also perfectly distinguished by some rank one separable measurement. Such a measurement may be written as

$$\{a_i a_i^* \otimes \bar{b}_i b_i^T : i = 1, \dots, N\}$$

for $a_1, \dots, a_N \in \mathcal{A}$ and $b_1, \dots, b_N \in \mathcal{B}$. As previously noted, we may assume without loss of generality that the vectors $a_i \otimes \bar{b}_i$ and $a_j \otimes \bar{b}_j$ are linearly independent for $i \neq j$. Based on the fact that this measurement perfectly distinguishes the elements in the chosen basis of \mathcal{Q} , we will determine that the basis

$$\left\{ u_1, \dots, u_{n^2-1}, \frac{1}{\sqrt{n}} \text{vec}(I_{\mathcal{B}, \mathcal{A}}) \right\}$$

of the entire space $\mathcal{A} \otimes \mathcal{B}$ diagonalizes each of the operators $Q(a_i a_i^* \otimes \bar{b}_i b_i^T)Q$ for $1 \leq i \leq N$. Because any two operators that are simultaneously diagonalized by a given basis must commute, we conclude that the operators $Q(a_i a_i^* \otimes \bar{b}_i b_i^T)Q$ and $Q(a_j a_j^* \otimes \bar{b}_j b_j^T)Q$ commute for every choice of i and j . However, based on the properties of the projection Q it can be shown that there must be a choice of i and j for which $Q(a_i a_i^* \otimes \bar{b}_i b_i^T)Q$ and $Q(a_j a_j^* \otimes \bar{b}_j b_j^T)Q$ do not commute. This is a contradiction that stems from the assumption that $\{u_1, \dots, u_{n^2-1}\}$ is an LOCC distinguishable basis of \mathcal{Q} , and so we conclude that such a basis does not exist.

We now give a more formal proof, beginning with a lemma that proves that there must exist choices of i and j for which the operators $Q(a_i a_i^* \otimes \bar{b}_i b_i^T)Q$ and $Q(a_j a_j^* \otimes \bar{b}_j b_j^T)Q$ do not commute.

Lemma 5. *Suppose that*

$$\{a_i a_i^* \otimes \bar{b}_i b_i^T : i = 1, \dots, N\}$$

is a rank one separable measurement such that $a_i \otimes \bar{b}_i$ and $a_j \otimes \bar{b}_j$ are linearly independent for all $i \neq j$. Then there exists a choice of i and j such that the operators

$$Q(a_i a_i^* \otimes \bar{b}_i b_i^T)Q \quad \text{and} \quad Q(a_j a_j^* \otimes \bar{b}_j b_j^T)Q$$

do not commute.

Proof. First note that as $\{a_i a_i^* \otimes \bar{b}_i b_i^\top : i = 1, \dots, N\}$ describes a measurement, we have

$$\sum_{i=1}^N a_i a_i^* \otimes \bar{b}_i b_i^\top = I_{\mathcal{A} \otimes \mathcal{B}}.$$

It follows that

$$\text{vec}(I_{\mathcal{B}, \mathcal{A}}) = \left(\sum_{i=1}^N a_i a_i^* \otimes \bar{b}_i b_i^\top \right) \text{vec}(I_{\mathcal{B}, \mathcal{A}}) = \text{vec} \left(\sum_{i=1}^N a_i a_i^* b_i b_i^* \right) = \text{vec} \left(\sum_{i=1}^N \langle a_i, b_i \rangle a_i b_i^* \right)$$

and therefore

$$\sum_{i=1}^N \langle a_i, b_i \rangle a_i b_i^* = I_{\mathcal{B}, \mathcal{A}}.$$

Taking the trace of both sides yields

$$\sum_{i=1}^N |\langle a_i, b_i \rangle|^2 = n.$$

Now, let

$$\alpha_{i,j} = (a_i^* \otimes b_i^\top) Q(a_j \otimes \bar{b}_j)$$

for all i, j . It will be proved that there exists a choice of $i \neq j$ such that $\alpha_{i,j} \neq 0$. In order to prove this, assume toward contradiction that $\alpha_{i,j} = 0$ for every pair $i \neq j$. As

$$\alpha_{i,j} = (a_i^* \otimes b_i^\top) Q(a_j \otimes \bar{b}_j) = \langle a_i, a_j \rangle \langle b_j, b_i \rangle - \frac{1}{n} \langle a_i, b_i \rangle \langle b_j, a_j \rangle,$$

we have that

$$\langle a_i, a_j \rangle \langle b_j, b_i \rangle = \frac{1}{n} \langle a_i, b_i \rangle \langle b_j, a_j \rangle$$

for all choices of $i \neq j$. Because $\sum_i |\langle a_i, b_i \rangle|^2 = n > 0$, we may choose some value of i for which $\langle a_i, b_i \rangle \neq 0$. We then have

$$\begin{aligned} \langle a_i, b_i \rangle &= a_i^* \left(\sum_j \langle a_j, b_j \rangle a_j b_j^* \right) b_i = \sum_j \langle a_j, b_j \rangle \langle a_i, a_j \rangle \langle b_j, b_i \rangle \\ &= \sum_{j \neq i} \langle a_j, b_j \rangle \langle a_i, a_j \rangle \langle b_j, b_i \rangle + \langle a_i, b_i \rangle \|a_i\|^2 \|b_i\|^2 \\ &= \frac{1}{n} \sum_{j \neq i} \langle a_j, b_j \rangle \langle a_i, b_i \rangle \langle b_j, a_j \rangle + \langle a_i, b_i \rangle \|a_i\|^2 \|b_i\|^2 \\ &= \left(\frac{1}{n} \sum_j |\langle a_j, b_j \rangle|^2 - \frac{1}{n} |\langle a_i, b_i \rangle|^2 + \|a_i\|^2 \|b_i\|^2 \right) \langle a_i, b_i \rangle \\ &= \left(1 - \frac{1}{n} |\langle a_i, b_i \rangle|^2 + \|a_i\|^2 \|b_i\|^2 \right) \langle a_i, b_i \rangle. \end{aligned}$$

As $\langle a_i, b_i \rangle \neq 0$ this implies

$$\frac{1}{n} |\langle a_i, b_i \rangle|^2 = \|a_i\|^2 \|b_i\|^2.$$

But then by the Cauchy-Schwarz Inequality we have

$$|\langle a_i, b_i \rangle|^2 \leq \|a_i\|^2 \|b_i\|^2 = \frac{1}{n} |\langle a_i, b_i \rangle|^2,$$

which implies $|\langle a_i, b_i \rangle|^2 = 0$. This contradicts the fact that i was chosen so that $\langle a_i, b_i \rangle \neq 0$, and so it has been proved that $\alpha_{i,j} \neq 0$ for some choice of $i \neq j$. Fix such a choice for the remainder of the proof.

Next, let us prove that the two vectors $Q(a_i \otimes \bar{b}_i)$ and $Q(a_j \otimes \bar{b}_j)$ are linearly independent. To this end let β and γ be scalars that satisfy

$$\beta Q(a_i \otimes \bar{b}_i) + \gamma Q(a_j \otimes \bar{b}_j) = 0.$$

This implies

$$\beta a_i \otimes \bar{b}_i + \gamma a_j \otimes \bar{b}_j = \frac{1}{n} (\beta \langle b_i, a_i \rangle + \gamma \langle b_j, a_j \rangle) \text{vec}(I_{\mathcal{B}, \mathcal{A}}),$$

or equivalently

$$\beta a_i b_i^* + \gamma a_j b_j^* = \frac{1}{n} (\beta \langle b_i, a_i \rangle + \gamma \langle b_j, a_j \rangle) I_{\mathcal{B}, \mathcal{A}}.$$

The left hand side of this equation has rank at most 2. Because we are assuming that $n \geq 3$ this means that the right hand side must be 0, for otherwise it would have rank $n \geq 3$. Thus $\beta a_i b_i^* + \gamma a_j b_j^* = 0$, which is equivalent to $\beta a_i \otimes \bar{b}_i + \gamma a_j \otimes \bar{b}_j = 0$. As $a_i \otimes \bar{b}_i$ and $a_j \otimes \bar{b}_j$ are necessarily linearly independent, however, this implies that $\beta = \gamma = 0$. Consequently $Q(a_i \otimes \bar{b}_i)$ and $Q(a_j \otimes \bar{b}_j)$ are linearly independent

To complete the proof, we must show that the two operators

$$Q(a_i a_i^* \otimes \bar{b}_i b_i^T) Q(a_j a_j^* \otimes \bar{b}_j b_j^T) Q = \alpha_{i,j} Q(a_i \otimes \bar{b}_i) (a_j^* \otimes b_j^T) Q$$

and

$$Q(a_j a_j^* \otimes \bar{b}_j b_j^T) Q(a_i a_i^* \otimes \bar{b}_i b_i^T) Q = \overline{\alpha_{i,j}} Q(a_j \otimes \bar{b}_j) (a_i^* \otimes b_i^T) Q$$

are not equal. Because $\alpha_{i,j} \neq 0$ and the vectors $Q(a_i \otimes \bar{b}_i)$ and $Q(a_j \otimes \bar{b}_j)$ are nonzero (as they are linearly independent), neither of these operators is 0. The images of the two operators are therefore the spaces spanned by the vectors $Q(a_i \otimes \bar{b}_i)$ and $Q(a_j \otimes \bar{b}_j)$, respectively. The fact that the two operators are not equal therefore follows from the linear independence of $Q(a_i \otimes \bar{b}_i)$ and $Q(a_j \otimes \bar{b}_j)$. \square

Proof of Theorem 4. The proof is by contradiction. To this end, assume $\{u_1, \dots, u_m\} \subset \mathcal{A} \otimes \mathcal{B}$, $m = n^2 - 1$, is an orthonormal basis of \mathcal{Q} whose elements are perfectly distinguished by some LOCC protocol. Then there exists a rank one separable measurement

$$\{a_i a_i^* \otimes \bar{b}_i b_i^T : i = 1, \dots, N\}$$

for which $a_i \otimes \bar{b}_i$ and $a_j \otimes \bar{b}_j$ are linearly independent for all $i \neq j$, together with a partition $S_1 \cup \dots \cup S_m = \{1, \dots, N\}$, $S_k \cap S_l = \emptyset$ for $k \neq l$, such that

$$u_k^* \left(\sum_{i \in S_l} a_i a_i^* \otimes \bar{b}_i b_i^\top \right) u_k = \delta_{kl}$$

for all $1 \leq k, l \leq m$.

Now, as

$$u_k^* (a_i a_i^* \otimes \bar{b}_i b_i^\top) u_k = |\langle u_k, a_i \otimes \bar{b}_i \rangle|^2,$$

it follows that u_k and $a_i \otimes \bar{b}_i$ are orthogonal whenever $i \notin S_k$. Consequently, it holds that

$$u_k^* (a_i a_i^* \otimes \bar{b}_i b_i^\top) u_l = 0$$

for $k \neq l$ given that S_k and S_l are disjoint. The projection Q acts trivially on each of the vectors u_1, \dots, u_m , and thus

$$u_k^* Q (a_i a_i^* \otimes \bar{b}_i b_i^\top) Q u_l = 0$$

for $k \neq l$. Letting $v = \frac{1}{\sqrt{n}} \text{vec}(I_{\mathcal{B}, \mathcal{A}})$ we obviously have $Qv = 0$, and thus

$$u_k^* Q (a_i a_i^* \otimes \bar{b}_i b_i^\top) Q v = v^* Q (a_i a_i^* \otimes \bar{b}_i b_i^\top) Q u_k = 0$$

for each choice of k as well. Thus, it has been shown that the orthonormal basis $\{u_1, \dots, u_m, v\}$ of $\mathcal{A} \otimes \mathcal{B}$ diagonalizes each of the operators $Q (a_i a_i^* \otimes \bar{b}_i b_i^\top) Q$, for $1 \leq i \leq N$. As these operators are all simultaneously diagonalized by a common orthonormal basis, they must therefore commute. However, by Lemma 5 this is not the case—for at least one choice of $i \neq j$ it holds that $Q (a_i a_i^* \otimes \bar{b}_i b_i^\top) Q$ and $Q (a_j a_j^* \otimes \bar{b}_j b_j^\top) Q$ do not commute. As a contradiction has been reached, this completes the proof of the theorem. \square

Impossibility for pairs of qubits

It should be noted that the assumption $n \geq 3$ in Theorem 4 is necessary. Indeed, every subspace of a tensor product space $\mathcal{A} \otimes \mathcal{B}$ where $\mathcal{A} = \mathbb{C}^2$ and $\mathcal{B} = \mathbb{C}^2$ has a perfectly distinguishable basis. To see this, let \mathcal{V} be a subspace of $\mathcal{A} \otimes \mathcal{B}$ and let $m = \dim(\mathcal{V})$. There is nothing to prove for $m = 0$ or $m = 1$, the claim for $m = 2$ follows from Walgate, et al. [14], and is trivial for $m = 4$. In the remaining case $m = 3$, it must be that \mathcal{V} is the orthogonal complement of some unit vector $u \in \mathcal{A} \otimes \mathcal{B}$. By considering the Schmidt decomposition of u , it is straightforward to find two product states $a_1 \otimes b_1$ and $a_2 \otimes b_2$ so that the set $\{u, a_1 \otimes b_1, a_2 \otimes b_2\}$ is orthonormal. Letting v be any vector orthogonal to the span of $\{u, a_1 \otimes b_1, a_2 \otimes b_2\}$, we have that $\{v, a_1 \otimes b_1, a_2 \otimes b_2\}$ is an orthonormal basis of \mathcal{V} . Walgate and Hardy [13] have shown that any such set is perfectly distinguishable given that at least two members of the set are product states.

4 Channels with suboptimal classical corrected capacity

Hayden and King [8] considered the classical capacity of quantum channels when the receiver has the capability to measure the channel's environment and to use the classical result of this measurement when measuring the output of the channel. In this section we give examples of channels that have suboptimal capacity with respect to this definition. In fact, the capacity of the channels remains suboptimal even when two-way communication is allowed between the receiver and the environment.

As our aim is to only prove the existence of channels with suboptimal classical corrected capacity rather than proving quantitative bounds on this capacity, we will use the following qualitative definition that does not refer to any specific measure of capacity. An admissible (i.e., completely positive and trace-preserving) mapping $\Phi \in \mathcal{T}(\mathcal{X}, \mathcal{A})$ is said to have *optimal two-way classical corrected capacity* if the following holds.

1. There exists a space \mathcal{B} and a unitary embedding $U \in \mathcal{L}(\mathcal{X}, \mathcal{A} \otimes \mathcal{B})$ such that

$$\Phi(X) = \text{tr}_{\mathcal{B}} UXU^*$$

for all $X \in \mathcal{L}(\mathcal{X})$, and

2. there exists an orthonormal basis $\{x_1, \dots, x_n\}$ of \mathcal{X} such that the set

$$Ux_1, \dots, Ux_n \in \mathcal{A} \otimes \mathcal{B}$$

is perfectly distinguishable by some LOCC protocol.

Note that by Proposition 3, a given mapping Φ fails to have optimal two-way classical corrected capacity if item 2 above fails to hold for even a single choice of U . This is because any other choice is equivalent up to a unitary operator on \mathcal{B} , which can simply be absorbed into the LOCC protocol.

The admissible maps that fail to satisfy the above definition are based on the subspaces considered in the previous section. Let $n \geq 3$, let $\mathcal{X} = \mathbb{C}^{n^2-1}$, and let $\mathcal{A} = \mathcal{B} = \mathbb{C}^n$. Choose $u_1, \dots, u_{n^2-1} \in \mathcal{A} \otimes \mathcal{B}$ to be an arbitrary orthonormal basis for the subspace \mathcal{Q} of $\mathcal{A} \otimes \mathcal{B}$. Define $U \in \mathcal{L}(\mathcal{X}, \mathcal{A} \otimes \mathcal{B})$ as

$$U = \sum_{i=1}^{n^2-1} u_i e_i^*.$$

Obviously U is a unitary embedding, so the mapping $\Phi \in \mathcal{T}(\mathcal{X}, \mathcal{A})$ defined by $\Phi(X) = \text{tr}_{\mathcal{B}} UXU^*$ for all $X \in \mathcal{L}(\mathcal{X})$ is admissible.

Corollary 6. *The mapping Φ does not have optimal two-way classical corrected capacity.*

Proof. If Φ were to have optimal two-way classical corrected capacity, there would be a choice of an orthonormal basis $\{x_1, \dots, x_{n^2-1}\}$ of \mathcal{X} such that $Ux_1, \dots, Ux_{n^2-1} \in \mathcal{A} \otimes \mathcal{B}$ is perfectly distinguishable by an LOCC protocol. As any such set is necessarily an orthonormal basis of \mathcal{Q} , this cannot be by Theorem 4. \square

Although the notion of correctable versus uncorrectable channels does not require that the input and output spaces have the same dimension, it is of course simple to adjust such an example to give a channel where this constraint is satisfied by viewing that the receiver's space \mathcal{A} is embedded in \mathcal{X} . One may therefore view the example above for $n = 3$ as giving a three-qubit channel having suboptimal two-way classical corrected capacity.

5 Conclusion

It has been proved that there exist subspaces of bipartite tensor product spaces that have no bases that can be perfectly distinguished by LOCC protocols, and this fact has been used to construct admissible mappings having suboptimal two-way classical corrected capacity. There are several interesting unanswered questions relating to these results, including the following.

1. What is the smallest dimension required for a subspace to have no bases perfectly distinguishable by LOCC protocols? (The smallest dimension achieved in the present paper is 8.)
2. Do there exist subspaces of $\mathcal{A} \otimes \mathcal{B}$ having no perfectly distinguishable bases when $\dim(\mathcal{A}) = 2$? As demonstrated in Section 3 this necessarily requires $\dim(\mathcal{B}) \geq 3$.
3. Quantitative bounds on the probability with which bases of the subspaces in question can be distinguished by LOCC protocols were not considered in this paper, and nor were specific bounds on classical corrected capacities of the associated channels. What can be proved about such bounds?

Acknowledgments

I thank Somshubhro Bandyopadhyay, Mehdi Mhalla, and Jonathan Walgate for several helpful discussions and suggestions. This research was supported by Canada's NSERC, the Canada Research Chairs program, and the Canadian Institute for Advanced Research (CIAR).

References

- [1] C. H. Bennett, D. P. DiVincenzo, C. A. Fuchs, T. Mor, E. Rains, P. W. Shor, J. A. Smolin, and W. K. Wootters, *Quantum nonlocality without entanglement*, Physical Review A **59** (1999), 1070–1091.
- [2] C. H. Bennett, D. P. DiVincenzo, T. Mor, P. W. Shor, J. A. Smolin, and B. M. Terhal, *Unextendible product bases and bound entanglement*, Physical Review Letters **82** (1999), 5385–5388.
- [3] P.-X. Chen and C.-Z. Li, *Orthogonality and distinguishability: criterion for local distinguishability of arbitrary orthogonal states*, Physical Review A **68** (2003), article 062107.

- [4] H. Fan, *Distinguishability and indistinguishability by local operations and classical communication*, Physical Review Letters **92** (2004), article 177905.
- [5] S. Ghosh, G. Kar, A. Roy, and D. Sarkar, *Distinguishability of maximally entangled states*, Physical Review A **70** (2004), article 022304.
- [6] S. Ghosh, G. Kar, A. Roy, A. Sen(De), and U. Sen, *Distinguishability of Bell states*, Physical Review Letters **87** (2001), article 277902.
- [7] M. Gregoratti and R. F. Werner, *On quantum error-correction by classical feedback in discrete time*, Journal of Mathematical Physics **45** (2004), no. 7, 2600–2612.
- [8] P. Hayden and C. King, *Correcting quantum channels by measuring the environment*, arXiv.org e-Print quant-ph/0409026, 2004.
- [9] M. Horodecki, A. Sen(De), U. Sen, and K. Horodecki, *Local indistinguishability: more non-locality with less entanglement*, Physical Review Letters **90** (2003), article 047902.
- [10] M. Nathanson, *Distinguishing bipartite orthogonal states using LOCC: best and worst cases*, arXiv.org e-Print quant-ph/0411110, 2004.
- [11] E. Rains, *Entanglement purification via separable superoperators*, arXiv.org e-Print quant-ph/9707002, 1997.
- [12] V. Vedral and M. B. Plenio, *Entanglement measures and purification procedures*, Physical Review A **57** (1998), 1619–1633.
- [13] J. Walgate and L. Hardy, *Nonlocality, asymmetry, and distinguishing bipartite states*, Physical Review Letters **89** (2002), article 147901.
- [14] J. Walgate, A. J. Short, L. Hardy, and V. Vedral, *Local distinguishability of multipartite orthogonal quantum states*, Physical Review Letters **85** (2000), 4972–4975.